THE HOMESOURCE, CORP.) Case No. 1:18-cv-11970
)
Plaintiffs,)
)
vs.)
)
RETAILER WEB SERVICES, LLC and)
JOHN DOES 1-3,)
Defendants.)
____________________________________)

Supplemental Declaration of Jennifer L. Bayuk, Ph.D.

March 11, 2019

On November 2, 2018, I was engaged in this matter on behalf of Retailer Web Services, LLC, ("RWS") as a computer security expert to opine on The HomeSource Corp.'s ("HomeSource") allegations in this case, which includes conducting an examination of HomeSource's evidence. My expertise in cybersecurity investigations began in the 1990s when I was a member of technical staff at Bell Laboratories. I was in a network security development group and was asked to advise Corporate Security on investigations that involved computers. Over the years, I accumulated investigation experience in various information security job functions, most prominently as Chief Information Security Officer for a major Wall Street firm. In that role, and several others, I was also responsible for systems security architecture, and I have designed detection, response, and recovery processes for multiple systems architectures, including architecture very similar to that operated by HomeSource. As an independent consultant, I leveraged my experience in conducting computer security investigations to earn a NJ Private Investigator's license. I also teach cybersecurity at the graduate level and wrote a textbook on CyberForensics. A full resume is in Attachment E of this declaration.

Table of Contents

A. *Background*

1. This declaration is submitted in response to a letter submitted by HomeSource on February 13, 2019 (Doc. No. 56) ("Letter").

2. I have reviewed the first and second amended complaints (Doc. No 12, Doc. No. 54-2) and HomeSource's discovery responses, including its responses to requests for admissions. I have actively participated in multiple meetings and email discussions in an attempt to identify and examine evidence in this case, as described in my previous declaration, Doc. No. 50-2 ("Declaration"). As I mentioned in that document, "Instead of examining evidence, I have primarily been so far engaged in coming to an agreement on the creation of a protocol by which both sides will share evidence and agree on the integrity of the output of a search." This statement remains true, as do all other statements in my Declaration.

3. The Letter contains a heading: "RWS's Expert Cannot Understand the Search Results without Obtaining Additional Information from HomeSource." (Doc. No. 56, PageID: 698.) This statement is capitalized for emphasis, as if communicating new information. In fact, it is trivially true. It is true because HomeSource has provided no description of its system of interest, but nevertheless has presented strings of characters that HomeSource claims are results of searches of logs from a system that has allegedly been attacked. "System of interest" is a term that system engineers use to distinguish a given system from all others with which it may be confused. A system of interest is defined by its distinguishing characteristics, i.e., what makes it recognizable to an outsider. To date, I have been provided with no information from HomeSource that would distinguish its system that was allegedly attacked from any other eCommerce system that utilizes Amazon Web Services.

B. *Industry Standards for Cybersecurity Investigations*

4. Computers are straightforward machines and computer security experts can assess how they work once they are provided with a list of components and a diagram specifying their interfaces. Computers follow straightforward logical algorithms based on electronic circuitry that speaks a language consisting of bits, that is, of ones and zeros, nothing more. Computer logs are automated messages that emanate from a wide variety of devices and applications. They typically include:
    a. a unique identifier for the source;
    b. a code that indicates whether attention to the message by a systems operator is urgent, given the activity detected at the source ("severity");
    c. the name and/or IP address of the server or other device on which the source software is processed (the "host");
    d. a timestamp that indicates when the activity occurred; and
    e. a message intended to be communicated to a systems operator by the author of the software.

    The message itself may have multiple fields, and combined they explain why the log was written. Most computing devices used by businesses come with logs preconfigured, so each business, in the course of constructing its systems environment, establishes a set of logs whether or not technology administrators have specifically configured them.

5. Guidelines for cybersecurity evidence collection have been established by the National Institute of Standards and Technology in its: *Guide to Integrating Forensic Techniques into*

Incident Response.[1] NIST recommends that computer forensic "*guidelines and procedures should support the admissibility of evidence into legal proceedings, including information on gathering and handling evidence properly, preserving the integrity of tools and equipment, maintaining the chain of custody, and storing evidence securely*" (NIST SP-800-86, p. 2-8). Procedures for data preservation are necessary to ensure that logs are available to be used by investigators in the event of an incident. Should an incident occur, industry standards instruct that several important steps should be taken. These are (NIST SP-800-86, p. 3-4):

a. develop and implement a plan to archive logs and other relevant data;
b. acquire and archive data specified by the plan;
c. verify the integrity of the data archived by computing a message digest (also known as a digital "fingerprint" because it uniquely identified a dataset) of both the original and archived data; and
d. document every step that was taken to collect the data, including information about each tool used in the process, in sufficient detail to allow others to repeat the process later if needed.

6. Technology industry standards for evidence collection and examination have been stable since the time of the NIST publication in 2006, and it is reasonable for me to expect that a party conducting a cybersecurity investigation would have gathered evidence that includes all log data from possibly relevant sources in four major data categories: files, operating systems, network traffic, and applications (NIST SP-800-86, pp. ES-1, ES-2).

C. HomeSource Deviation from Industry Standards

7. In my Declaration, I stated that I based my first proposal for a shared protocol for evidence examination on the industry standard approach to cybersecurity forensics as described by NIST. That Declaration describes the reaction of HomeSource, specifically that HomeSource considered it unnecessary to follow industry standards. The Declaration states: "*Although the assumptions and steps in the protocol were taken directly from the agreements during the meeting on November 14, HS counsel Arena instead proposed that the search be conducted solely by HS using a search tool she described as a 'crude query.' The crude query allowed entry of IP addresses and output of IP addresses, without addressing any of the industry standard steps in my draft protocol*" (Doc. No. 50-2, PageID: 612-613). The Declaration also observed: "*At that meeting, Arena also informed us that the web server log data set was so large it was not practical to reproduce it, and that she would get back to us on how it was preserved*" (Doc. No. 50-2, PageID: 620).

8. On December 19, HomeSource's expert, Kevin Tuten, informed me that a copy of the HomeSource web log server had been made using Amazon Web Services snapshots. We discussed how to perform an examination of the evidence chain of custody in that context. I sent him a diagram and few screenshots from my own Amazon Web Services environment to illustrate a feasible approach. These are in Attachment A. Tuten sent return email with redacted screenshots of the Home Source log copy process, showing the steps followed by HomeSource within Amazon Web Services. An excerpt from that email is in Attachment B. In the email, Tuten asks me to "double check that HS didn't miss anything needed for Chain of Custody." At the time, I responded verbally that we would have several issues with the emailed chain of custody demonstration:

[1] NIST Special Publication (SP) 800-86 (2006), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

a. we had no system diagram nor configuration of log sources, so we did not have a method to verify that logs were sent to the original server;

b. the name of the original server identifier was redacted on the screenshots, so we would not be able to tell what data was copied to the device in the screenshot; and

c. the screenshots show that the copy occurred on December 7, so we did not have the method by which log integrity was preserved between August and December.

To date, the web application logs have not been made available to me. I have no update on a method by which the chain of custody issues may be addressed.

D. Lack of Evidence

9. Section 1 of the Letter states that: "*HomeSource has already produced to RWS (in September and December 2018) evidence of the cyberattacks that it may introduce at trial and the documents that HomeSource relies on to support its allegations in the complaint.*" (Doc. No. 56, PageID: 697.) That statement has no basis in any evidence made available to me. I have seen no actual logs, nor evidence that there is a chain of custody or preservation of integrity between the alleged logs and the alleged search results.

10. As of Friday March 8, 2019 and as emphasized in footnote 1 of the Letter (Doc. No. 56, PageID: 697), the only evidence that had been made available in this case was:

a. a set of extracts from web log records alleged to be output from searches on HomeSource web server logs using IP addresses as search input ("Search Hits"); and

b. a subpoena to GoDaddy with a list of IP addresses with no explanation of what investigation was done to produce the list.

On Friday, March 8, 2019, HomeSource sent an email to RWS counsel with an additional claim of evidence in documents that displayed a set of malformed URLs and a screenshot of the search software in use. None of the IP addresses in the documents delivered on March 8 belong to RWS and none were the same as those previously delivered in the Search Hits or GoDaddy subpoena.

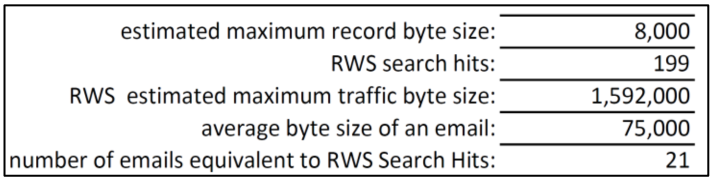
11. The only mention in case materials that I have found for the origin of the Search Hits was in the *Certification of James White in Support of the Plaintiff's Opposition to Defendant's Motion to Seal* (filed on February 19, 2019, Doc. No. 58-1) ("White Certification"). In that document, White states that HomeSource subpoenaed four companies for IP addresses associated with the user account of James Kane (Vimeo in paragraph 5, LinkedIn in paragraph 9, Google in paragraph 10, and Cox in paragraph 22). Concerning the Search Hits, White writes: "HomeSource was then instructed to search our logs for this IP address, so that the associated data could be produced to RWS's counsel in discovery. We did so." (White Certification paragraph 7). Note that the White Certification identifies only one IP address, but the Search Hits file RWS received based on that search contains 157 unique addresses. Although two others are recognizable to RWS Counsel as IP Addresses attributable to the home network James Kane and Jennie Gilbert at that time. HomeSource has provided no claim of evidence that the other 154 IP Addresses in the Search Hits file represent activity conducted by RWS. In the Search Hits for August 2018, only 199 are attributable to RWS. This level of traffic is consistent with market research activity in which RWS admits to have been engaged.

12. Footnote 1 of the Letter refers to a Distributed Denial of Service (DDoS) attack (Doc. No. 56, PageID: 697). A DDoS attack is accomplished by consuming network or system

resources, typically by sending large amounts of data that overwhelms computing resources. Technology industry standards for investigating DDoS attacks make use of network device logs. Where a DDoS attack is aimed at a web server (such as that owned by HomeSource), the Multi-State Information Sharing and Analysis Center advises DDoS investigators to look for patterns of malicious traffic as follows: "*An HTTP GET Flood occurs when an attacker, or attackers, generate a significant number of continuous HTTP GET requests for a target website in an attempt to consume enough resources to make the server unavailable for legitimate users. In this case, the attacking IP addresses never wait for a response from the target server, despite the server attempting to respond to all incoming requests. This results in connections being left open on the web server*."[2] The document then advises to "*investigate network logs and look for a large number of inbound traffic from a significant number of source IP addresses*."

13. HomeSource has claimed such disruption at the hands of RWS, and has also claimed that it is not possible to separate malicious traffic from non-malicious traffic in their logs. The industry standard term DDoS does not refer to a method of causing unspecified damage that cannot be identified as malicious. Nevertheless, Section 1 of the Letter states that HomeSource logged 6 million records and 99% of them are not relevant to the case. (Doc. No. 56, PageID: 696.) That implies that HomeSource has determined that ~60,000 of its records are relevant to the case, but there are no indications of an investigation that revealed that this number of records are malicious, not even in the form of an approximation. As noted above, a DDoS attack is characterized by an attempt to overwhelm system resources. If one were to assume that there had been a DDoS attack that made use of 60,000 website requests that could not be distinguished from normal traffic, then the size of each request would have to be indistinguishable from the size of a normal web server request. There is no fixed limit on web server requests, but there is an observed maximum size accepted by many web servers of ~8,000 bytes.[3] If we were to assume (i) a generous size estimate of 8,000 bytes per "normal" request and (ii) all of the RWS IP records in the Search Hits for August 2018 were attempts to maximize computing resource consumption (199), then RWS would have consumed only 1,592,000 bytes, or 1.5MB (See Figure 1). This is not enough data to overwhelm the computing resources of a typical eCommerce web server. For comparison's sake, the size of an average email is 75KB.[4] Assuming 8,000 bytes for each of the 199 visits attributed to RWS in August 2018, this means the alleged RWS traffic volume is the equivalent of ~21 emails. HomeSource has not presented any method or evidence by which RWS's attributable traffic could have caused the alleged DDoS. Indeed, HomeSource has not presented any evidence that any of the RWS visits to its customers' websites have caused any damage or disruption of any kind.

Figure 1: Example Estimated Maximum Size of RWS Traffic



estimated maximum record byte size:	8,000
RWS search hits:	199
RWS estimated maximum traffic byte size:	1,592,000
average byte size of an email:	75,000
number of emails equivalent to RWS Search Hits:	21

[2] Myers, L. (2017). Guide to DDOS Attacks. (Doc. No. 31, PageID: 290; see also https://www.cisecurity.org/wp-content/uploads/2017/03/Guide-to-DDoS-Attacks-November-2017.pdf, Multi-State Information Sharing and Analysis Center, p. 10).

[3] See for example: https://stackoverflow.com/questions/2659952/maximum-length-of-http-get-request.

[4] See: https://www.lifewire.com/what-is-the-average-size-of-an-email-message-1171208.

14. Section 1 of the Letter states that there is evidence of attacks in a subpoena to GoDaddy. (Doc. No. 56, PageID: 697, footnote 1.) I reviewed both that subpoena (Doc. No. 59-1) and its response (there is no document number on the GoDaddy response, so I have attached it to this report as Attachment C). The data in the subpoena is a list of timestamps and IP addresses. None of the IP addresses belong to RWS and none of them appear in the Search Hits. GoDaddy's response to the subpoena stated simply that they "were unable to locate any specific user level request associated to the activity." Nevertheless, in its Second Amended Complaint, HomeSource claims that: "GoDaddy has informed HomeSource that GoDaddy cannot identify John Doe, because the GoDaddy account was compromised at the time the attacks occurred." (Doc. No. 54-2, paragraphs 59-60.) There is a very big difference between "unable to locate any specific user level request" and "account was compromised." According to GoDaddy's written response, GoDaddy did not even associate the activity with any account, much less identify an account that was compromised. The statement that there is evidence of attacks in the subpoena to GoDaddy has no basis in any evidence made available to me.

15. In the Second Amended Complaint, HomeSource claims that: "*Through discovery, HomeSource learned that RWS designed and deployed software ("spiders" or "web crawlers") to monitor and download information from HomeSource's websites for the purpose of disrupting HomeSource's business and to gain an unfair competitive advantage*." (Doc. No. 54-2, paragraph 57). However, the only evidence that contains a reference to spider activity is a device type field in the Search Hits. In August 2018, there was one record that included both an RWS IP address and a device type: spider. The timestamp on that record is August 13, three days after the alleged start of the first DDoS attack. Use of a spider program to inspect ("crawl") a competitor website is a common occurrence on the Internet and is consistent with market research activity admitted by HomeSource. HomeSource has provided no evidence linking this record or any item identified in discovery to a "purpose of disrupting HomeSource's business and to gain an unfair competitive advantage."

E. Concessions on Industry Standards

16. Section 3 of the Letter claims a causal connection between the format of HomeSource web logs and the difficulty of coming up with a search protocol. (Doc. No. 56, PageID: 698.) My description of my efforts to agree on a search protocol in my Declaration never once mentioned expected difficulty in performing a web log search. Again, I am a systems architect, programmer, and analyst with three decades of experience. I am not daunted by unfamiliar technology. Data structures are not mysterious objects, they are simply methods of organizing sets of bits.

17. In fact, I was directed by RWS counsel to make as many concessions as I could in order simply to gain assurance that the data jointly searched by the experts would be recognizably the same if it was searched by HomeSource at a later date. That is, RWS withdrew all requirements to follow industry standards for connecting the data to a system of interest, and withdrew all requirements for proof of a data custody chain from that systems of interest in the interest of reaching a compromise to allow a joint search for RWS IP addresses in HomeSource logs. RWS was interested in simply capturing a digital fingerprint of the searched logs and results so I could prove that subsequent searches of the same logs in the same manner would yield the same result.

18. As I described in my Declaration, the situation that led to a conversation with Jim White was not related to the search tool. It was prompted by the fact that the draft protocol at that time specified that the joint search would be done with both experts in the *same physical location*. Because HomeSource would not allow me to have direct access to the data, we compromised on being in the same room with the person doing the search. This was to enable me to oversee the search and the production of the data integrity fingerprint with minimal concern that the IP list would be compromised or the search environment altered without my knowledge. The relevant excerpt from my Declaration is (Doc. No. 50-2, PageID: 612-613): "*However, again the document was rejected by HS. Tuten let me know that he thought a major issue was the cost of his travel to the NJ offices of HS's counsel. He set up a call with Jim White of HS for later that afternoon."* I did not volunteer to travel to Tuten's office in FL because the case is venued in NJ, and Tuten expressed a willingness to travel. Had HomeSource funded Tuten's trip to NJ, we could have executed the search as previously agreed.

19. In my Declaration, I described the conversation with White as follows (Doc. No. 50-2, PageID: 612-613): "*I explained to Jim* <White> *that my only objective in being physically present during the search was to have information on which I could opine. I explained that if I had no direct access to the environment under scrutiny, I could not personally opine to the validity of any actual evidence, just to the fact that I saw images on screen that could have been produced via PowerPoint and that any opinion I gave would be the equivalent of saying that I watched a movie. But if I could see how the machines were interacting and could have the ability to type commands and queries myself, I could collect enough information to determine how the technology was actually working, and thereby be able to endorse the validity of the search result. At first White objected that, as agent of RWS, I could not be trusted not to steal trade secrets that may be stored in the search environment…."* White agreed on the phone to the final protocol that I then drafted, but withdrew his agreement later without explanation. I was told that the protocol was rejected, but not, as described in Section 3 of the Letter, because it was "*unworkable*." Again, how computers "work" is not a mystery. HomeSource had previously told me that their search tool was Amazon Elastic Search. The protocol included a statement that HomeSource would teach Tuten and me how to use the search tool, but that was not an admission on my part that I could not figure out how to use Amazon Elastic Search. Logs of this type are not complex nor complicated. My submission to training was made because of hesitation on the part of HomeSource to allow me to use the search tool at all. White expressed concern that our query results may not work. Hence it was agreed both experts would use the search tool after preliminary instruction.

F. Explanation of HomeSource Productions

20. The screenshot provided in HomeSource's Friday, March 8 production reveals the existence of an industry standard, user-friendly, and well-known search tool, [redacted], that is being used to search HomeSource's logs. This existence of this query facility lays to rest the notion that the data would be hard to interpret, as claimed in Section 3 of the Letter.

21. HomeSource made it difficult to agree on a protocol because they resisted sharing any information about the system of interest and the source of the logs, and did not to allow me to directly examine its evidence. This is the equivalent of a medical doctor being asked to opine on a patient's condition without access to either the patient or the medical chart. To think that anyone would be able to understand results from a log search although they have not been given information describing the system of interest would be equivalent to asking a doctor to

evaluate a patient's health based on the patient's weight, with no corresponding information on the patient's physical condition, height, metabolism, or medical history. This is true even though there is nothing as mysterious about computer operation as there is about human biology.

22. The evidence provided by HomeSource has so far been equivalent to a claim that a patient has been adversely impacted by a fever of 98.7 degrees Fahrenheit because 98.6 is the established average, though in fact what is normal for any given person can range from 97 to 99.[5] This analogy is intended to communicate that HomeSource has sent data in the March 8 production that looks slightly unusual, but in isolation is not known to be directly correlated with poor systems health. It is my experience, and that of my peers and graduate students, that once a website is published on the Internet, it immediately becomes the target of cyberattack. It used to be the case that a professor had to cause malicious activity in order for a student to observe it. Now, we just wait for the attacks to occur. Even if there was malicious activity directed specifically against HomeSource, it is not reasonable to expect that such evidence would be recognizable as a targeted attack without context. Moreover, because the data is unconnected with a description of its source, it is as if a patient's temperature was delivered to a medical expert without disclosing any description of the patient's physiology, any other symptoms, known prior conditions, results of medical examinations performed, whether or not any blood tests or other diagnostics were run, nor allowing the expert to see the patient, read the chart, or calibrate the thermometer. A statement that the computer output disclosed in this case is connected with damage to an unseen system has just as little basis as the claim that the slightly elevated fever has caused significant medical impact to an unseen patient. The admission that the search results cannot be understood without explanation to be provided by the plaintiff is an admission that evidence has been withheld or was not captured by HomeSource.

23. Section 3 of the Letter quotes a section of my Declaration concerning an initial analysis of the Search Hits wherein I wrote that there was: "*no evidence of any IP address in the log accessing any site as an authorized user*;" and "*no evidence of hiding IP addresses*" (Doc. No. 50-2, PageID: 631). The Letter calls my words "*baseless*." In fact, these words are based on my knowledge of how web servers typically produce and store logs, in combination with technology industry standards for forensic evidence. Specifically, web server logs store requests made by users, but not the response to the request. By design, they do not expose the application logic behind the request processing. The additional explanation needed to understand what underlying activity is represented by a web log would be a detailed diagram of how the web request is interpreted and processed by a business software application. The business application software would typically query a database before providing a response back to the web server, which in turn passes data to the user. A simplified version of such a control flow is called a "message sequence diagram," because it refers to the content and sequence of information expected to be passed between integrated systems. An example of a message sequence diagram is included in Attachment D. From this type of diagram, it is clear that a business software application may also produce logs which would be relevant to interpreting the strings of data in a web server request passed to it.

24. Section 3 of the Letter also implies that, although there is no way to separate benign from malicious traffic in the logs, a HomeSource employee will be able to make a determination that the logs show malicious activity. (Doc. No. 56, PageID: 698.) There is a statement that

[5] See https://www.mayoclinic.org/first-aid/first-aid-fever/basics/art-20056685.

"RWS apparently thinks that there is no 'smoking gun.'" The statement implies that a HomeSource employee *can* see a smoking gun. The Letter acknowledges that a HomeSource employee could link a website request that contains an IP address to malicious behavior, and that the explanation may be expected to be provided in a deposition. This is inconsistent with HomeSource's repeated claim that there is no way to separate benign from malicious traffic in their logs. If an employee can explain why a log entry represents malicious activity, then both the complete set of log entries that correspond to the activity, and the evidence that the employee relies upon in the explanation can be produced. I can only conclude that HomeSource's refusal to share its alleged evidence is the reason why I am unable to independently recognize what they see as malicious traffic in the data strings associated with RWS IPs, unless such malicious traffic does not exist.

G. *Consequences of HomeSource's Lack of Evidence*

25. If RWS were to follow the advice in Section 3 of the Letter to ask a "*HomeSource employee to sit down in a deposition and walk RWS's counsel and RWS's expert through the RWS IP search results line by line, and explain what they mean*," then that employee would be asked to describe the forensic evidence preservation plan, the archived data chain of custody, the data flow between systems processing malicious requests, and describe the logs that would have been revealed in the joint search that was anticipated to occur in discovery. Questions would be asked about the ingress network traffic route that is directed to the network port on which the web server is configured to listen, the functionality of the program identified in the request URL, the input expected to be posted by the user to the program and how it differs from the input in normal traffic (if at all), a description of the application that processed the request in the log record, the response to the request (to include any negative impact that HomeSource experienced in the course of processing the request), and the network egress paths by which data is provided back to the requestor. If HomeSource has documented its systems data flow and forensics investigation process, then the answers to most of these questions could have been provided in response to the discovery request for: "All documents relied upon by HomeSource to support its allegations in the Complaint."

    Most importantly, the explanation would include a description of damage to HomeSource caused by one or more malformed or otherwise malicious web requests. The admission that this explanation is necessary to enable RWS to properly interpret the evidence is also an admission that there is evidence missing from HomeSource's production of its discovery.

26. The lack of a clear specification on what constitutes malicious traffic is the reason why RWS does not want to disclose its full list of IP addresses. Unless the disclosure can be done in conjunction with a method of digitally fingerprinting (i) searched logs and (ii) results of searches using those IP addresses, then there would be no method to verify the integrity of the searched logs, and the logs could be altered after the IP addresses are disclosed.

27. The RWS resistance to disclose its IP address list is also justified by its claim that its business will be impacted by having to replace its confidential IP addresses once disclosed. Even though some may think, as Jim White claims in the White Certification, "*it costs pennies (little to no money) for a company like RWS to obtain a new IP address*," but any change to technology impacting network configuration requires careful planning, and every technology change costs something. When IP addresses change that support production systems, work must be done to ensure there is no impact to business data flow while the

change is made, and the change requires testing and coordination that often must be scheduled for times of low volumes like weekends or Holidays.

H. Summary

28. All this said, the most fundamental flaw with HomeSource's claim that it has suffered a cyberattack is the lack of evidence based on industry standards for the collection and preservation of forensic evidence. These instruct: "*Before the analyst begins to collect any data, a decision should be made by the analyst or management (in accordance with the organization's policies and legal advisors) on the need to collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings.... If it is unclear whether or not evidence needs to be preserved, by default it generally should be preserved.*" (NIST SP-800-86, p. 3-4.) To date, I have been presented with no evidence that any usual and customary steps to collect and preserve evidence have been performed by HomeSource. Mishandling and tampering issues remain unaddressed. HomeSource's failure to substantiate the integrity of its data, coupled with its continued mantra that there is "no way to separate the benign from the malicious traffic," leaves no reasonable basis upon which HomeSource may claim evidence of malice.

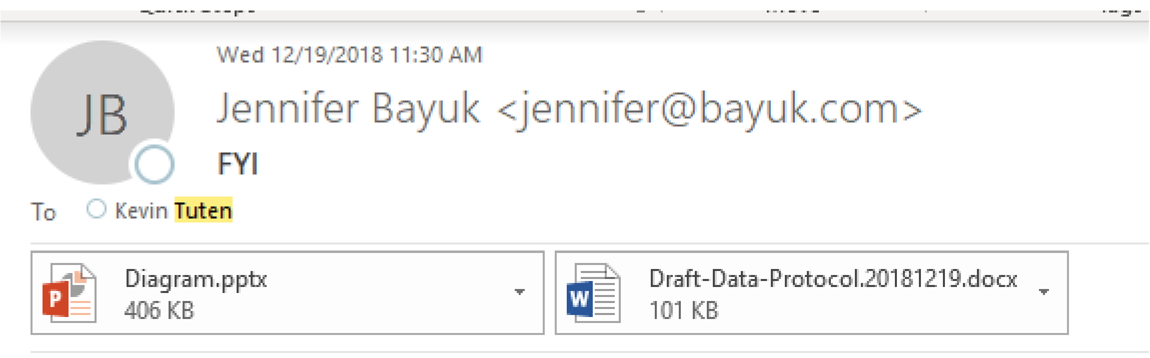
29. It in incongruous that HomeSource claims to have produced evidence of damage from the alleged cyberattacks when the fundamental facts of the alleged attacks have not been disclosed. I do not know *which* website or websites were allegedly attacked, specifically *when* a given website was allegedly attacked, *how* any website was allegedly attacked, nor *what* harm was done to the confidentiality, integrity, or availability of data or services provided by the website(s). The only information HomeSource has provided unequivocally is *who* they accuse of allegedly initiating an attack, that is: RWS. However, none of the IP addresses that HomeSource identified in its subpoena to GoDaddy and in its March 8 production match RWS's IP address list. In the Search Hits, only three of the IP addresses correspond to RWS IP addresses, for which there is a reasonable explanation. If HomeSource has configured logs with the intent to record cyberattacks, then the logs should contain clues with which to deduce the answers to the questions I have about which, when, how and what. Therefore, it is important for me to understand the system configuration and log configuration, and to examine the complete set of messages logged during the alleged attacks, in addition to any other evidence HomeSource has of the alleged attacks.

I declare under the penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 11th Day of March, 2019.

Jennifer L. Bayuk, Ph.D.

Attachment A: Excerpt of Email to Tuten with Example Data Preservation Evidence



Wed 12/19/2018 11:30 AM

Jennifer Bayuk <jennifer@bayuk.com>

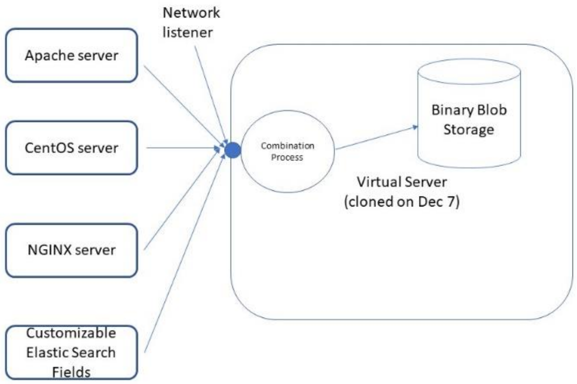
FYI

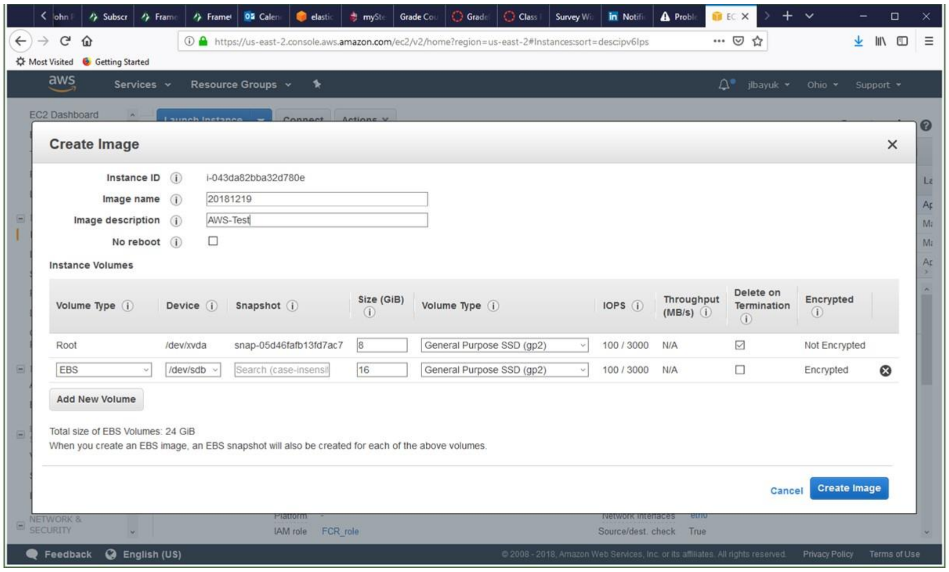
To ○ Kevin Tuten

Diagram.pptx 406 KB

Draft-Data-Protocol.20181219.docx 101 KB

Standing by…




https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:sort=desc:ipv6Ips
Most Visited
Getting Started
aws
Services
Resource Groups
jlbayuk
Ohio
Support
EC2 Dashboard
Launch Instance
Connect
Actions
NETWORK & SECURITY
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Create Image

Instance ID: i-043da82bba32d780e

Image name: 20181219

Image description: AWS-Test

No reboot: □

Instance Volumes

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-05d46fafb13fd7ac7	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted
EBS	/dev/sdb	Search (case-insensit	16	General Purpose SSD (gp2)	100 / 3000	N/A	□	Encrypted

Add New Volume

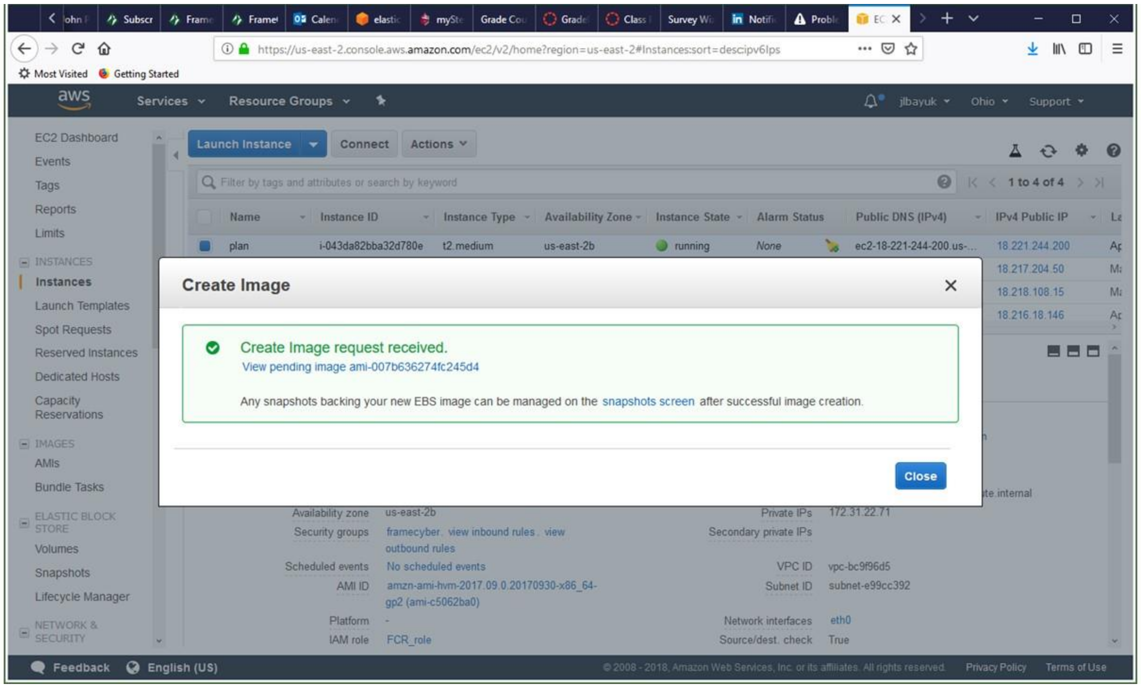
Total size of EBS Volumes: 24 GiB

When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

Cancel | Create Image

IAM role FCR_role

Source/dest. check True



Name	Instance ID	Instance Type	Availability Zone	Instance State	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	La
plan	i-043da82bba32d780e	t2.medium	us-east-2b	running	None	ec2-18-221-244-200.us-...	18.221.244.200	Ap
							18.217.204.50	Ma
							18.218.108.15	Ma
							18.216.18.146	Ap

Create Image ×

Create Image request received.

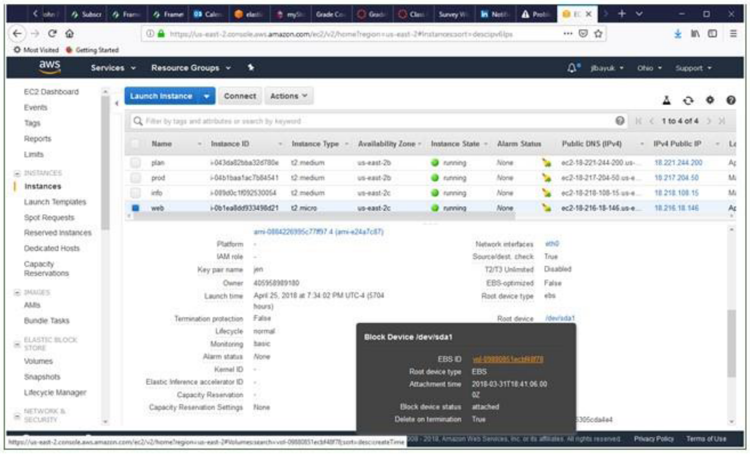
View pending image ami-007b636274fc245d4

Any snapshots backing your new EBS image can be managed on the snapshots screen after successful image creation.

Close

Availability zone us-east-2b
Security groups framecyber. view inbound rules. view outbound rules
Scheduled events No scheduled events
AMI ID amzn-ami-hvm-2017.09.0.20170930-x86_64-gp2 (ami-c5062ba0)
Platform -
IAM role FCR_role

Private IPs 172.31.22.71
Secondary private IPs
VPC ID vpc-bc9f96d5
Subnet ID subnet-e99cc392
Network interfaces eth0
Source/dest. check True



Name	Instance ID	Instance Type	Availability Zone	Instance State	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	La
plan	i-043da82bba32d780e	t2.medium	us-east-2b	running	None	ec2-18-221-244-200.us-...	18.221.244.200	Ap
prod	i-04b1baa1ac7b84541	t2.medium	us-east-2b	running	None	ec2-18-217-204-50.us-e...	18.217.204.50	Ma
info	i-089d0c1f092530054	t2.medium	us-east-2c	running	None	ec2-18-218-108-15.us-e...	18.218.108.15	Ma
web	i-0b1ea8dd933498d21	t2.micro	us-east-2c	running	None	ec2-18-216-18-146.us-e...	18.216.18.146	Ap

ami-0884226995c77ff97.4 (ami-e24a7c87)
Platform -
IAM role -
Key pair name jen
Owner 405958989180
Launch time April 25, 2018 at 7:34:02 PM UTC-4 (5704 hours)
Termination protection False
Lifecycle normal
Monitoring basic
Alarm status None
Kernel ID -
Elastic Inference accelerator ID -
Capacity Reservation -
Capacity Reservation Settings None

Network interfaces eth0
Source/dest. check True
T2/T3 Unlimited Disabled
EBS-optimized False
Root device type ebs
Root device /dev/sda1

Block Device /dev/sda1

EBS ID vol-09880851ecbf48f7f
Root device type EBS
Attachment time 2018-03-31T18:41:06.000Z
Block device status attached
Delete on termination True

5305cda4e4

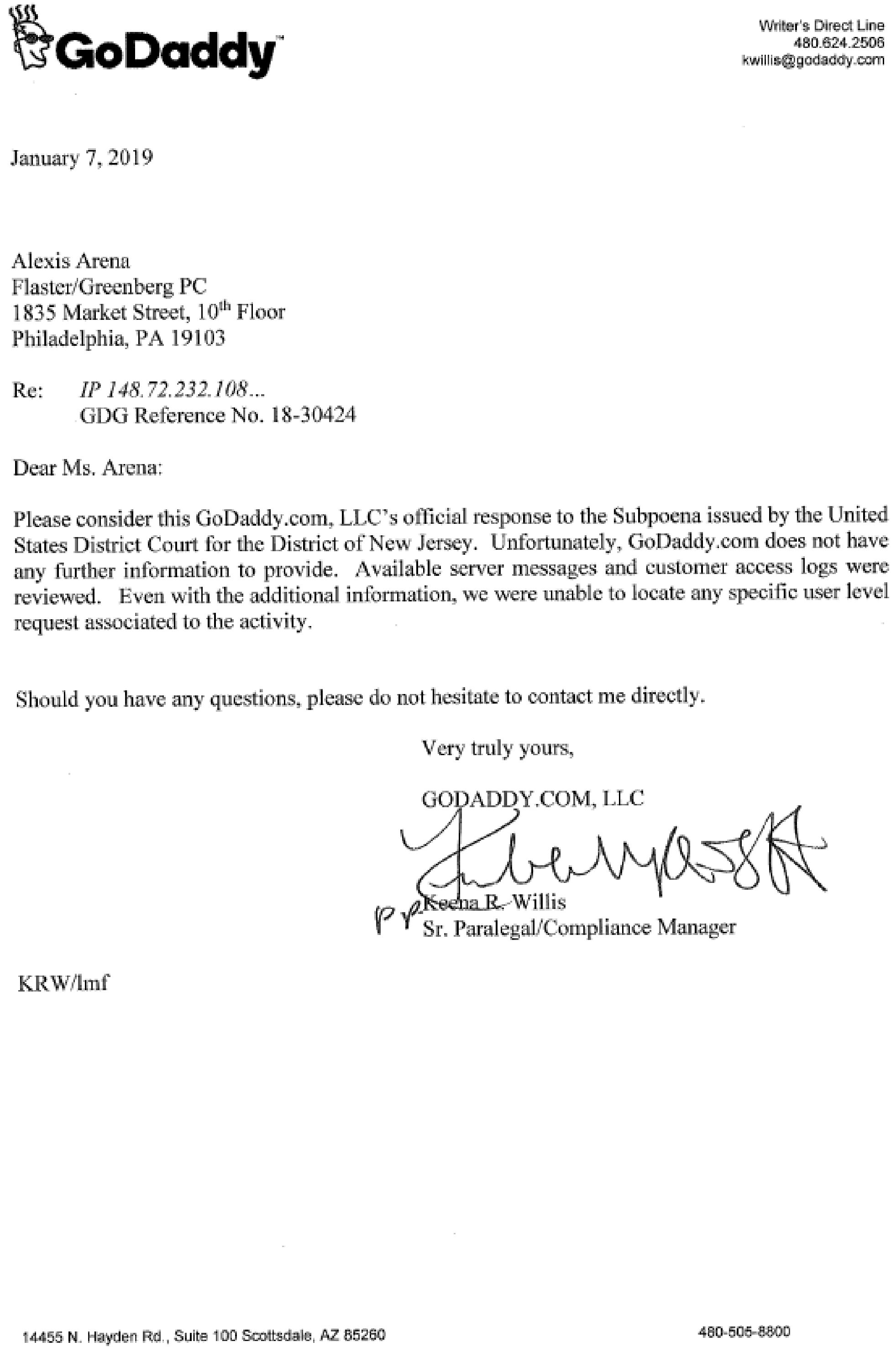
https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Volumes:search=vol-09880851ecbf48f7f;sort=desc:createTime

Example from checking old snapshot to see where it came from – looking at volumes

Attachment B: Excerpt of Email From Tuten with HomeSource Screenshots

[redacted]

Attachment C: GoDaddy Response to Subpoena in Doc. 59 Ex. 1



GoDaddy

Writer's Direct Line
480.624.2506
kwillis@godaddy.com

January 7, 2019

Alexis Arena
Flaster/Greenberg PC
1835 Market Street, 10th Floor
Philadelphia, PA 19103

Re: *IP 148.72.232.108…*
GDG Reference No. 18-30424

Dear Ms. Arena:

Please consider this GoDaddy.com, LLC's official response to the Subpoena issued by the United States District Court for the District of New Jersey. Unfortunately, GoDaddy.com does not have any further information to provide. Available server messages and customer access logs were reviewed. Even with the additional information, we were unable to locate any specific user level request associated to the activity.

Should you have any questions, please do not hesitate to contact me directly.

Very truly yours,

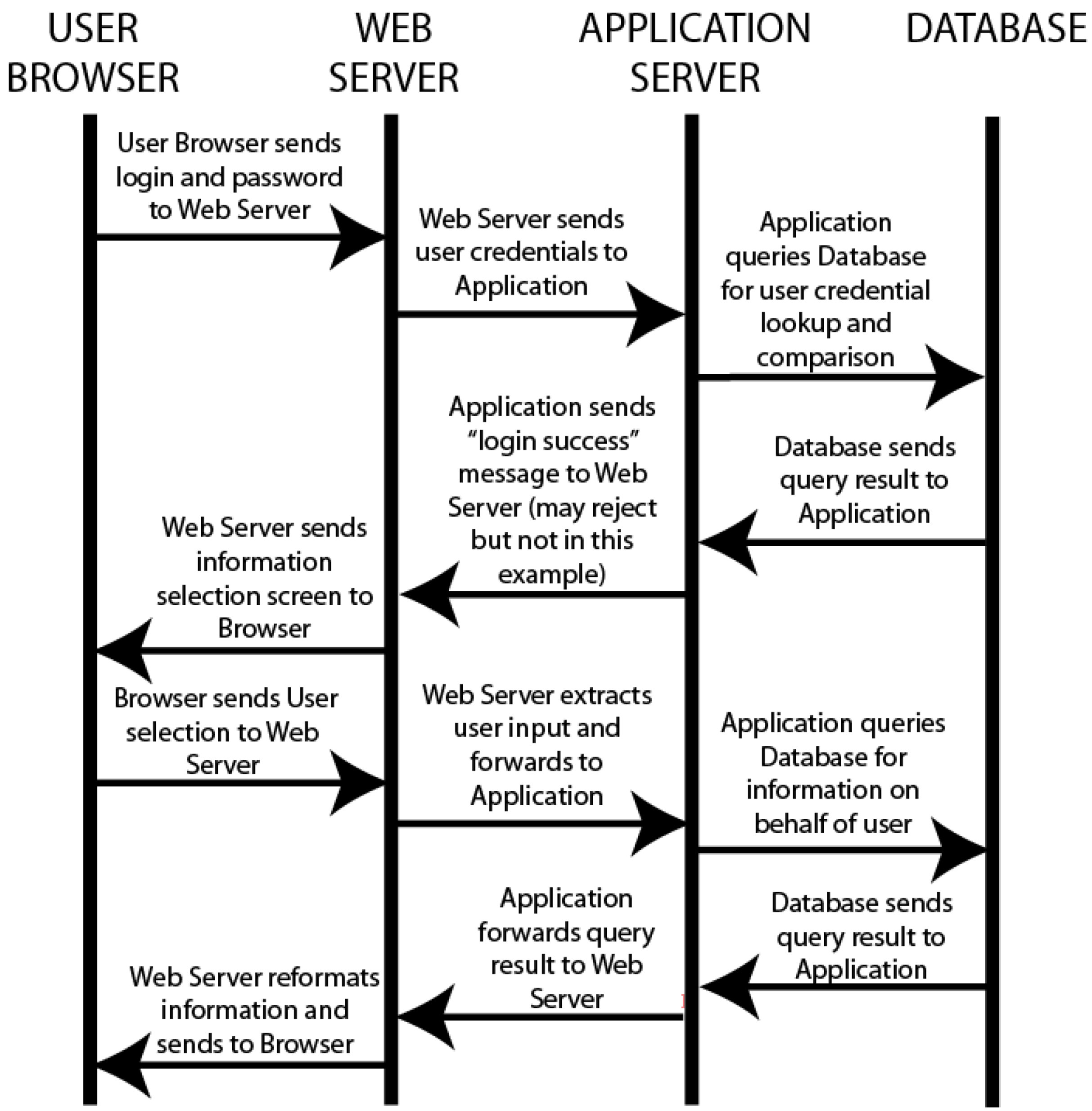
GODADDY.COM, LLC

pp Keena R. Willis
Sr. Paralegal/Compliance Manager

KRW/lmf

14455 N. Hayden Rd., Suite 100 Scottsdale, AZ 85260 480-505-8800

Attachment D: Example Message Sequence Diagram


USER BROWSER
WEB SERVER
APPLICATION SERVER
DATABASE
User Browser sends login and password to Web Server
Web Server sends user credentials to Application
Application queries Database for user credential lookup and comparison
Database sends query result to Application
Application sends "login success" message to Web Server (may reject but not in this example)
Web Server sends information selection screen to Browser
Browser sends User selection to Web Server
Web Server extracts user input and forwards to Application
Application queries Database for information on behalf of user
Database sends query result to Application
Application forwards query result to Web Server
Web Server reformats information and sends to Browser

Attachment E: Bayuk Resume

JENNIFER L. BAYUK

PROFILE Experienced in leading, managing and measuring large-scale technology risk management programs. Skilled in system security architecture, cloud security strategies, information security tools and techniques, cybersecurity forensics, audit of information systems and networks, technology risk and performance indicators, security risk awareness education, risk management training curriculum, and systems engineering research. Masters degrees in Philosophy and Computer Science. Ph.D. in Systems Engineering. Certified in Information Systems Audit, Information Systems Security, Information Security Management, and IT Governance. NJ Licensed Private Investigator.

EDUCATION

PhD Systems Engineering, Stevens Institute of Technology, 2012, Thesis: Measuring Systems Security, GPA 3.9.
MS Computer Science, Stevens Institute of Technology, 1992, GPA 3.9.
MA Philosophy, The Ohio State University, 1986, GPA 3.5.
BA Computer Science & Philosophy, Rutgers College, Rutgers, the State University of NJ, 1985, GPA 3.59.

CERTIFICATIONS

Certified Information Systems Auditor (CISA), 1996+
Certified Information Security Manager (CISM), 2002+
Certified in the Governance of Enterprise IT (CGEIT), 2008+
Certified Information Systems Security Professional (CISSP), 2008-2013.

TECHNOLOGY

Software Architecture: Current: Cloud Applications with Multi-tier Security, Past: Including but not limited to: Three-tier Web applications, Third Party Risk Management Systems, Identify and Access Management Systems, Software inventory and Control Systems, Expert Systems for Telecommunications Maintenance
Programming Language: Current: Java, Python, Linux shell, Past: Including but not limited to: C, C++, C#, LISP
Tools: Including but not limited to: Report writers in API and GUI interfaces, Various SDLC Tools, Vitech CORE and similar systems engineering tools, Encase and similar forensics tools, WireShark and similar network analysis tools, SSH, RDP, Citrix, and other remote access tools, Adobe Suite, Visio, Camtasia, MS Office, Google Docs
Databases: MongoDB, Oracle, PostgreSQL, MySQL, Sybase, Access
Cloud Administration: AWS, GCP, O365
Operating Systems: Linux, Windows, ChromeBook, past: OS390, iSeries, Solaris, AIX
Business Applications: I have operated and administered dozens of business data automation applications, and frequently served as business data owner to ensure technical specifications met business requirements

BOOKS

December 2018	*Financial Cybersecurity Risk Management,* coauthor, Springer Apress.
April 2012	*Cyber Security Policy Guidebook*, as lead of five authors, combined different areas of cybersecurity policy expertise into a comprehensive guide, Wiley.
September 2010	*CyberForensics, Understanding Information Security Investigations*, edited this collection of articles by industry experts and provided an introductory framework, Springer.
January 2010	*Enterprise Security for the Executive: Setting the Tone at the Top*, Praeger.
March 2009	*Enterprise Information Security and Privacy*, Artech House, co-edited this collection of srticles, and wrote chapter on "Information Classification."
November 2007	*Stepping Through the InfoSec Program*, Information Systems Audit and Control Association (ISACA), internationally peer-reviewed book.
January 2005, 2000	*Stepping Through the IS Audit, A Guide for Information Systems Managers, 2nd Edition*. Book published by ISACA and peer-reviewed. 1st Edition published in January 2000

Cybersecurity Risk Management Consultant, New Jersey, 6/08 to present

Engaged in a wide variety of projects ranging from policy and metrics for financial institutions to research in systems security engineering for government contractors. Develop systems security architecture. Perform cybersecurity risk and regulatory compliance assessments. Develop and teach courses in various aspects of cybersecurity for academic institutions and industry associations. Lecture at conferences. Participate in public and private security-related committees. Assist entrepreneurs on Cybersecurity Architecture, Technology Risk Management, and secure Cloud and Mobile requirements. Provide expert witness and legal consulting services. Exemplar projects:

Quinnipiac University, Hamden, CT, 1/19-present.
Created a new graduate laboratory course in Operating Systems Security for the School of Engineering, including instruction on how to create virtual operating systems in Amazon Web Services, to administer. Linux and Apache Web Server Security, and conduct forensics investigations in the Amazon Cloud. Created plan to establish a cloud-based cybersecurity laboratory. Current adjunct professor.

Stevens Institute of Technology, Hoboken, NJ, 9/09-present.
Created a new graduate curriculum in cybersecurity for the School of Systems and Enterprises, including four new courses in systems security architecture and engineering. Led research projects in systems security engineering, including a research roadmap for the Department of Defense Systems Engineering Directorate. Created a systems security engineering laboratory. Current adjunct professor.

Decision Framework Systems, Towaco, NJ, 01/18-present.
Designed, developed, and implemented FrameCyber, a complete cybersecurity risk management life cycle system. FrameCyber is a cloud software product designed to be used continuously with full retention of data and actions. It includes functions for cybersecurity risk assessment, event tracking, issue management, organization inventory, control inventory, risk registration, risk analysis, risk reporting, risk measures and metrics, and associated correlation of information and data in those domains required to perform cybersecurity risk management. Manage all aspect of the company, including legal, finance, customer support, marketing and engineering.

Information Systems Audit and Control Association (ISACA), 3/09-present.
Develop and teach courses on emerging topics in cybersecurity and technology risk and controls.

Institute for Defense Analysis, Washington, D.C., 6/18
Cybersecurity subject matter expert participant in an initiative to maintain the U.S. science and technology advantage in air defense of the Nation, “Air Force Science and Technology Strategy 2030.” The initiative was administered by Institute for Defense Analysis for the Air Force Research Laboratory.

G. A. Baird Partners & Co, Stamford, CT, 6/17-11/17.
Created Cybersecurity and Technology Risk tools, techniques, and programs for a *de novo* peer-to-peer Bank. Specified systems security architecture for Digital Banking Architecture and Third Party Integration, focused on Cloud and Mobile Security Technologies.

Delta Risk, Chicago, IL, 7/09-1/13.
Provided business requirements, testing, and analysis for Securities Industry and Financial Markets Association (SIFMA) Quantum Dawn Cybersecurity Exercises. Assisted in the development of DECIDE simulation environment for experiencing cyber attack scenarios, and the scenarios used by SIFMA.

Managing Director, Cybersecurity Governance, Risk &Control, JPMorgan Chase, NY, NY, 10/16 to 6/17.
Designed, managed, and measured a Cybersecurity Risk Management framework in support of $600M Firmwide Cybersecurity Program. Managed the evolution of cybersecurity and technology risk policies and standards in coordination with cybersecurity product managers and the broader Technology Control organization. Globally coordinated cybersecurity regulatory, audit, client, and partner engagement in coordination with Technology Control and Cybersecurity Regional leads. Managed firmwide governance and control processes applicable to the Cybersecurity organization, including but not limited to risk and control self-assessment, resiliency and recovery, issue management, third party oversight, and inter-affiliate agreements.

Managing Director, Operational Risk Management, Citi, New York, NY, 3/13 to 10/16.
Coordinated activities within first and second lines of defense to identify, measure, monitor, and manage key operational risks within Citi’s Enterprise Operations and Technology (O&T) division in accordance with firmwide Policies and Procedures. Defined roles and responsibilities, developed procedures, guidelines, and training to support forward-looking risk identification, address control weaknesses, leverage best practices, and enforce consistent risk containment throughout the firm. Proactively engaged individuals at all levels of management to understand and assess both inherent and residual risk due to business dependency on technology and centralized operations such as Human Resources and Financial Services. Participated in risk-related forums such as the firm’s Information Security Committee, Fraud Oversight Committee, and Business Risk and Control forums. and tracked issues. Devised and directed the development of Technology Oversight Procedures and Technology Metrics used firmwide for BASEL management control assessment and operational risk analysis.

Senior Managing Director, CISO, Bear Stearns & Co., Inc., Whippany, NJ, 4/98 to 6/08.
Designed and implemented firmwide processes to protect, detect, and recover from harm to information. Devised tools, techniques, roles, responsibilities, and awareness materials for all security processes including digital identity, application inventory and cybersecurity incident investigation. Established and maintained

enterprise-wide security, change control, and business continuity metrics. Chair of the Firmwide Information Protection Committee and member of the Global Outsourcing and Firmwide Emergency Response Committees. Issued global security policies and processes. Provided technical requirements and test programs for new security products and security features of new applications. Directed information security investigations and remediation activities in coordination with human resources, legal and compliance. Coordinated emergency response teams for information security related events. Reviewed physical security efforts in support of data center protection. Contracted and managed penetration tests. Guided management through information technology (IT) audits. Performed due diligence in support of merger, acquisition, research analyst, and investment banking activity. Testified on due diligence efforts when required by regulators. Directly managed department budget (~3M) and security tollgates over all projects in IT budget (~600M).

Manager, Information Systems Business Controls, AT&T Capital Corporation, Morristown, NJ, 2/97 to 4/98.
Led and executed the company's global internal audit and control assessments with respect to information systems. Conducted security investigations. Provided direction and guidance on systems control issues for the company's strategic leaders, including the Technology Leadership Team and corporate legal counsel. Developed COSO & COBIT compliant systems audit approach for AT&T Capital that includes quantitative communication of systems vulnerabilities. Evaluated and developed tools for operating system, database management system, and network security testing as well as data analysis, incident tracking, and reporting.

Information Systems Risk Manager, Price Waterhouse LLP, Morristown, NJ, 1995 - 1997.
Managed a wide variety of security consulting and audit projects for the Price Waterhouse Information Systems Risk Management Practice, including penetration tests and physical infrastructure reviews. Performed systems infrastructure analysis directed at improving technical security architecture, security management processes, and information system operational risk management. Developed methodology for evaluating the effectiveness of security management processes and trained both consultants and senior managers on its use. Wrote and customized programs for security testing. Evaluated various types of commercial security software.

Information Security Technical Staff, AT&T Bell Laboratories, Holmdel, NJ, 1990 - 1995.
Led diverse, cross-organizational teams focused on security and data integrity, including the AT&T Network Security Requirements Team, the Security Analysis of the Network Environment Team, and the Security Assessment Team. Envisioned, designed, specified, developed, demonstrated, tested, and documented software for expert systems, graphical user interfaces, databases, and network monitors. Spent most of the last year at AT&T with the CFO Organization in Short Hills performing computer security audits and corporate security consulting for various systems comprising and supporting the AT&T Worldwide Intelligent Network.

Courses Developed, Listed By Initial Launch

February 2018	*Operating System Security in Amazon Web Services,* Lab Course at Quinnipiac University
September 2018	*Risk Management for Financial Cybersecurity,* Stevens Institute of Technology
June 2018	*Technology's Role in Enterprise Risk Management,* ISACA, NJ Chapter
June 2015	*Loss Capture for Technology-Related Events,* Citigroup Internal Online Training.
January 2015	*Technology Oversight Procedures,* Citigroup Internal Online Training.
August 2014	*Manager's Control Assessment,* Citigroup Internal Online Training.
June 2014	*Information Security Architecture,* Citigroup Internal Online Training.
November 2013	*Information Security Metrics,* Citigroup Internal Online Training.
March 2012	*System Security Management,* Univ of Virginia's Accelerated Master's in Systems Engineering.
June 2012	*Information Security Governance at Board Level*, seminar for ISACA & IIA NJ Chapters.
April 2012	*Security Documentation*, ISACA Philadelphia & New Jersey Chapters Spring Conference.
Spring 2011	*Systems Security Architecture and Design,* Stevens Institute of Technology
Spring 2011	*Fundamentals of Security Systems Engineering,* Stevens Institute of Technology
Spring 2011	*Secure Systems Laboratory*, Stevens Institute of Technology
June 2010	*Metrics That Actually Improve Security*, Computer Security Institute.
Spring 2009	*Secure Systems Foundations,* Stevens Institute of Technology
March 2009	*Information Security Metrics,* ISACA, NY Chapter
March 2009	*Information Security Governance,* ISCACA, NJ Chapter
January 2009	*Information Asset Classification*, ISACA, NY Chapter.
April 1998	*CISA Exam Certification Course*, Domain 4: Information Systems Integrity, Confidentiality, and Availability, ISACA North Jersey Chapter (Also taught in April 1999 and April 2000).

More details and select articles & speaking engagements

Available at http://www.bayuk.com